**Le Règlement Général sur la Protection des Données**

**Version du 7 mars 2021**

**Auteur : Karine Roobrouck**

Le Règlement général sur la protection des données (RGPD) est désormais en vigueur depuis près de 3 ans. Les entreprises ont eu le temps de se conformer à ses exigences et l'Autorité de protection des données a déjà remis plusieurs avis.

En guise de rappel...

## 1. INTRODUCTION

Le RGPD est un règlement du Parlement européen et du Conseil (Règlement (UE) 2016/679) immédiatement applicable dans tous les États membres. Cela signifie que, contrairement aux directives européennes, toutes les dispositions du règlement sont directement contraignantes et qu'il ne doit donc pas être préalablement transposé en droit national.

Avant le RGPD, il existait la *directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*. Toutefois, comme il s'agissait d'une directive et pas d'un règlement, chaque État membre devait la transposer dans son droit national. Cela a donné lieu à une fragmentation de la législation et à divers niveaux de protection dans les différents États membres, ce qui n'était finalement pas favorable à la sécurité juridique.

En outre, les progrès technologiques fulgurants et la mondialisation nous confrontent à de nouveaux défis en matière de protection des données à caractère personnel. Le législateur européen a voulu satisfaire ces besoins. Les objectifs de la directive 95/46/CE demeurent intacts, mais le nouveau règlement vise à créer un cadre cohérent et homogène.

Le RGPD est applicable depuis le 25 mai 2018. La directive 95/46/CE a été abrogée ce même jour.

## 2. DONNÉES À CARACTÈRE PERSONNEL

### 2.1. Généralités

Le règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

L'on entend par « données à caractère personnel » :

> *« toute information se rapportant à une personne physique identifiée ou identifiable (la « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »*

L'on entend par « traitement » :

*« toute opération ou tout ensemble d'opérations effectuées **ou non** à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »*

L'on entend par « fichier » :

*« tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique »*

Le RGPD est donc d'application à votre administration en tant qu'entrepreneur, ainsi qu'à votre fichier de clientèle, votre comptabilité… et peut-être même au contenu de vos traductions, si celles-ci contiennent des données à caractère personnel.

Le règlement concerne cependant uniquement les données de personnes physiques. Cela signifie qu'il ne s'applique pas aux données de personnes morales (une S.P.R.L., une S.A., une A.S.B.L., etc.). Par contre, cela signifie que vous êtes, en tant qu'entrepreneur/personne physique, également protégé par le RGPD.

### 2.2 Données à caractère personnel sensibles

Les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, les données génétiques, les données biométriques, les données concernant la santé, ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique peuvent uniquement être traitées :

- avec le consentement explicite de la personne concernée ; ou
- si le traitement est nécessaire à la constatation, à l'exercice ou au fondement d'une action en justice.

(Le RGPD énumère d'autres possibilités qui ne sont, à mon avis, pas pertinentes pour le secteur de la traduction.)

### 2.3. Condamnations pénales et infractions

Le traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions ne peut être effectué :

- que sous le contrôle de l'autorité publique ; ou
- si le responsable du traitement fournit des garanties appropriées pour les droits et libertés des personnes concernées.

Une garantie appropriée pourrait, par exemple, être l'obligation de discrétion et le secret professionnel auxquels vous êtes tenus en tant que traducteurs et interprètes jurés.

Constituent par exemple des données à caractère personnel :

- Les données de localisation (adresse IP, tracking...)
- Les informations relatives au comportement (loisirs, intérêts...)
- Les convictions (religion, opinions politiques, appartenance syndicale...)
- Les données concernant la santé (données médicales/génétiques)
- Les données financières (informations bancaires, mais aussi patrimoine)

- Les données sociales et juridiques (origine raciale ou ethnique, condamnations...)
- Les données professionnelles
- Les données biométriques
- Les données comportementales (orientation sexuelle...)
- ...

## 3. LE SOUS-TRAITANT ET LE RESPONSABLE DU TRAITEMENT

Le RGPD établit une distinction claire entre le sous-traitant et le responsable du traitement. Tous deux peuvent être des personnes physiques ou morales.

- Le « responsable du traitement » est la personne qui détermine les finalités et les moyens du traitement de données à caractère personnel.

- Un « sous-traitant » est une personne qui traite effectivement les données à caractère personnel.

Ces définitions sont importantes pour une bonne compréhension de vos obligations.

Lorsque le sous-traitant et le responsable du traitement sont deux personnes différentes, le RGPD leur impose de conclure un contrat écrit par lequel le sous-traitant offre des garanties suffisantes pour protéger les droits de la personne concernée et s'engage à respecter les instructions du responsable du traitement.

Si le sous-traitant souhaite à son tour faire appel à un autre sous-traitant, ce deuxième sous-traitant doit également signer un contrat. Le recrutement d'un autre sous-traitant est subordonné à l'autorisation expresse préalable du responsable du traitement.

## 4. LES PRINCIPES DU TRAITEMENT

Le traitement des données à caractère personnel doit satisfaire aux exigences suivantes :

- Le traitement doit être loyal et disposer d'un fondement légitime (voir point 5 ci-après).

- Les données à caractère personnel doivent être collectées pour une finalité déterminée, explicite et légitime (limitation des finalités) ; les données collectées pour une finalité déterminée ne peuvent pas être utilisées à d'autres fins.

- Minimisation des données : le traitement des données à caractère personnel ne peut pas dépasser le cadre nécessaire ; vous ne pouvez pas collecter des données *« sous prétexte qu'elles peuvent toujours être utiles »*. L'idéal est de recueillir le moins de données possible.

- Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour.

- Les données à caractère personnel ne peuvent pas être conservées plus longtemps que nécessaire.

- Les données à caractère personnel doivent être protégées de manière appropriée contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle.

## 5. LE FONDEMENT LÉGITIME

Le traitement des données doit disposer d'un fondement légitime parmi ceux cités ci-dessous. Vous pouvez traiter des données à caractère personnel :

- avec le consentement de la personne concernée ;
- pour exécuter un contrat ;
- pour respecter une obligation légale ;
- pour protéger les intérêts vitaux d'une autre personne ;
- pour exécuter une mission d'intérêt public ou exercer l'autorité publique ;
- pour défendre les intérêts légitimes du responsable du traitement ou d'un tiers.

## 6. LES DROITS DE LA PERSONNE CONCERNÉE

Les droits de la personne concernée reposent en grande partie sur le fondement légitime.

- **Droit à l'information :** la personne concernée doit être informée, dans un langage compréhensible (cf. déclaration de transparence ci-après), de ses droits au moment où des données à caractère personnel sont collectées. Le responsable du traitement des données veille également à ce que la personne concernée puisse exercer ces droits sans problème.

- **Droit d'accès :** une suite doit être réservée dans le mois à toute demande d'une personne concernée désireuse d'exercer son droit d'accès. Si la personne concernée en fait la demande, une copie doit également lui être remise.

- **Droit de rectification et d'effacement des données :** la personne concernée dispose d'un droit de rectification de ses données à caractère personnel inexactes et incomplètes. La personne concernée dispose également du droit à l'oubli. Pour autant qu'elles ne doivent plus être conservées dans le but pour lequel elles ont été collectées, les données à caractère personnel seront effacées à la demande de la personne concernée.

- **Droit à la limitation du traitement :** dans certaines circonstances, la personne concernée peut demander de limiter le traitement des données.

- **Droit à la portabilité des données :** si le traitement est fondé sur le consentement et s'il est effectué à l'aide de procédés automatisés, la personne concernée peut demander que ses données à caractère personnel soient transmises à un autre responsable du traitement.

## 7. TRANSPARENCE

Si vous obtenez des données à caractère personnel, faites connaître à la personne concernée ses droits. Deux scénarios sont possibles :

### 7.1 Les données sont collectées auprès de la personne concernée

Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, une série d'informations.

Mieux vaut donc, si des informations vous sont communiquées dans le but de vous permettre de faire offre, retourner votre devis accompagné d'une déclaration de transparence.

La déclaration de transparence doit être simple, claire et concise, ce qui ne sera pas chose aisée, compte tenu de l'abondance de renseignements à fournir :

- l'identité et les coordonnées du responsable du traitement ;

- les finalités et le fondement légitime du traitement ;
- les éventuels destinataires ou catégories de destinataires des données à caractère personnel (si vous travaillez avec des sous-traitants, par exemple) ;
- le cas échéant, votre intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou une organisation internationale (un traducteur sis en dehors de l'Union européenne, par exemple) ;
- la durée précise de conservation des données ;
- l'existence du droit de réclamer au responsable du traitement la rectification ou l'effacement des données, ou une limitation du traitement, et du droit à la portabilité des données ;
- le droit dont dispose la personne concernée de retirer son consentement à tout moment ;
- le droit d'introduire une réclamation auprès de la l'Autorité de protection des données ;
- des informations sur l'exigence de fourniture de données à caractère personnel (A-t-elle un caractère réglementaire ou contractuel, conditionne-t-elle la conclusion d'un contrat ? La personne concernée est-elle tenue de fournir les données à caractère personnel ? Quelles seraient les conséquences d'une absence de fourniture des données ?)

Si vous avez déjà communiqué ces informations précédemment à la personne concernée, vous n'avez pas à les lui répéter.

Si vous disposez d'un site Internet, d'une page Facebook ou d'un profil LinkedIn, la déclaration de transparence peut y être évoquée.

### 7.2 Les données n'ont pas été collectées auprès de la personne concernée

Lorsque les données à caractère personnel n'ont pas été collectées auprès d'elle, le responsable du traitement fournit à la personne concernée les informations suivantes :

- l'identité et les coordonnées du responsable du traitement ;
- les finalités et le fondement légitime du traitement ;
- les catégories de données à caractère personnel concernées ;
- les éventuels destinataires ou catégories de destinataires des données à caractère personnel ;
- le cas échéant, votre intention d'effectuer un transfert de données à caractère personnel vers un destinataire sis dans un pays tiers ou vers une organisation internationale ;
- la durée précise de conservation des données ;
- l'existence du droit de réclamer au responsable du traitement la rectification ou l'effacement des données, ou une limitation du traitement, et du droit à la portabilité des données ;
- le droit dont dispose la personne concernée de retirer son consentement à tout moment ;
- le droit d'introduire une réclamation auprès de la l'Autorité de protection des données ;
- la source des données à caractère personnel.

Ces informations doivent être fournies dans le mois qui suit l'obtention des données à caractère personnel ou, si celles-ci doivent être utilisées pour communiquer avec la personne concernée, au plus tard au moment de la première communication à cette personne.

Elles n'ont pas à l'être :

a) si la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés, auquel cas le responsable du traitement prendra des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée ;
b) si l'obtention ou la communication des informations sont expressément prévues par la loi, et que le droit prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée ; ou

c) si les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel.

## 8. REGISTRE DES ACTIVITÉS DE TRAITEMENT

Chaque sous-traitant et chaque responsable du traitement devront tenir un registre des activités de traitement de données effectuées sous leur responsabilité.

Cette obligation s'applique également aux PME, notamment concernant la gestion des clients et l'administration du personnel. Ce registre doit être écrit, mais une version électronique est suffisante. En cas de contrôle de l'Autorité de protection des données, il sera le premier élément de preuve que vous vous vous conformez au RGPD.

Ce registre est un fichier qui doit vivre. Sa tenue représente un surcroît de travail, mais je vous conseille de l'intégrer dès le début à votre administration de manière systématique, même si le risque d'un contrôle est minime. Il suffit d'un client mécontent pour déclencher un contrôle.

Que doit contenir précisément ce registre ?

### 8.1 Le registre du responsable du traitement

- le nom et les coordonnées du responsable du traitement ;
- les finalités du traitement ;
- les catégories de personnes concernées ;
- les catégories de données à caractère personnel ;
- les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ;
- dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

### 8.2 Le registre du sous-traitant

- le nom et les coordonnées des sous-traitants et de chaque responsable du traitement pour le compte duquel agit le sous-traitant ;
- les catégories de traitements effectués pour le compte de chaque responsable du traitement ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

Indiquez, en outre, dans votre registre si vous avez informé ou non la personne concernée sur le traitement de ses données. La mention de cette information dans le registre n'est pas obligatoire, mais elle peut vous aider à démontrer que vous vous conformez au RGPD.

Des modèles de registre sont disponibles sur le site Internet de l'Autorité de protection des données et seront également diffusés par la CBTI.

## 9. SÉCURITÉ

Le responsable du traitement et le sous-traitant doivent mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir la sécurité des données à caractère personnel. Ces « mesures appropriées » ne sont actuellement pas clairement définies, mais le RGPD précise :

> *« compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques »*

Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle (p. ex., plantage informatique) ou illicite (vol, piratage, etc.).

Le responsable du traitement et le sous-traitant sont responsables de toute personne qui agit sous leur autorité et qui a accès à des données à caractère personnel. Par conséquent, il vous est conseillé de conclure un contrat de sous-traitance avec votre sous-traitant dans lequel vous exigez qu'il mette en œuvre des mesures appropriées.

## 10. NOTIFICATION D'UNE FUITE DE DONNÉES

Vous êtes tenu(e) de notifier toute fuite de données à la suite d'un vol, d'un virus, d'un piratage, etc.

### 10.1 Notification à l'autorité

Si vous êtes confronté(e) à une fuite de données, vous devez la notifier à la Commission de la protection de la vie privée 72 heures au plus tard après en avoir pris connaissance, à moins que cette fuite de données ne soit pas susceptible d'engendrer un risque pour les droits et libertés de la personne concernée.

### 10.2 Communication à la personne concernée

Lorsque la fuite de données est susceptible d'engendrer un risque élevé pour les droits et libertés de personnes physiques, vous devez également la communiquer à la personne concernée, à moins que cette fuite ne porte sur des données rendues inaccessibles ou incompréhensibles pour des tiers (p. ex. chiffrement) ou que vous n'ayez pris des mesures ultérieures qui garantissent que le risque n'est plus susceptible de se matérialiser.

Cette obligation peut se révéler une tâche ardue, par exemple si vous vous faites voler votre ordinateur, votre tablette ou votre smartphone qui contenait tout votre fichier clients. Les personnes morales ne doivent pas être informées d'une fuite de données, car elles ne sont pas protégées par le RGPD.

**Que devez-vous faire ?**

1. Dressez la liste des catégories de données à caractère personnel que vous traitez, et définissez les finalités de ces traitements. Vérifiez que vous ne collectez pas plus de données que nécessaire au regard des finalités définies. Supprimez les données à caractère personnel dont vous n'avez plus besoin.
2. Assurez-vous que le traitement des données à caractère personnel s'appuie sur un fondement légitime. Si ce fondement relève du « consentement », vérifiez que celui-ci satisfait aux critères imposés par le règlement.
3. Joignez la déclaration de transparence à tout devis adressé à la personne concernée. Si les données ont été collectées auprès d'un tiers, voyez s'il y a lieu d'informer la personne concernée.

4. Établissez un registre des activités de traitement, et tenez-le soigneusement à jour.
5. Signez des contrats de sous-traitance avec tous vos partenaires.
6. Protégez au mieux vos fichiers.
7. Signalez toute fuite de données.